August 3, 2022

VIA ELECTRONIC MAIL

Chairwoman Jessica Rosenworcel
Federal Communications Commission
45 L Street, N.E.
Washington, DC 20554
Jesssica.Rosenworcel@fcc.gov

Re: Letter of Inquiry to T-Mobile dated July 19, 2022.

Dear Chairwoman Rosenworcel:

Thank you for the opportunity to respond to your Letter of Inquiry of July 19, 2022 ("Inquiry").

Let me start by emphasizing that T-Mobile recognizes that we must earn and keep our customers' trust by respecting and protecting their privacy. Of course, we must collect and retain data to provide our services to consumers—both the core services, including E911, and additional services that our customers value. In doing so, T-Mobile adheres to core privacy principles, including:

- Trust – valuing privacy of the data entrusted to us, and remaining loyal to that trust;
- Transparency – providing openness and honesty about T-Mobile's privacy practices;
- Control – putting consumers in control with clear, simple data choices and helping our customers understand privacy and data use so that they can make the right choices; and
- Protection – enabling tools to help keep customers' data protected.

Applying these principles, T-Mobile has designed our stewardship of customer information with privacy at the forefront. T-Mobile's Privacy Center provides a single location for consumers to view both T-Mobile's Privacy Notices and explanations of the privacy tools and choices T-Mobile makes available to its customers. Also, as we develop new programs and features, we follow CTIA's Best Practices and Guidelines for Location-Based Services and employ a privacy-by-design approach, while ensuring advancement of our core privacy principles.

As our responses below demonstrate, T-Mobile's Geolocation Data collection, retention, disclosure, and security practices comply with FCC requirements,[1] other applicable state and federal data protection laws, and industry best practices. Our responses to your questions follow.

Requests for Information

1.a. *Please describe in detail the geolocation data that T-Mobile and Metro collect and/or retain regarding current and/or former subscribers. How is that data collected?*

Like all wireless providers, T-Mobile (including Metro) collects several different types of location information to provide our commercial mobile radio ("CMRS") and commercial mobile data service ("CMDS"), including internet access service. For example, we collect information about a customer's location when they place or receive cell phone calls or text messages, or when they have an active data session. T-Mobile's responses to your questions specifically address our collection, retention, and protection of Geolocation Data, which is location data that (1) relates to an identified or reasonably identifiable person, (2) identifies an individual's location within 1,850 feet, which is the largest distance considered "sensitive" or "precise" under state laws,[2] (3) T-Mobile collects by providing domestic CMRS and CMDS to individuals, and (4) T-Mobile collects solely by virtue of the carrier-customer relationship.[3]

T-Mobile collects three types of Geolocation Data. First, T-Mobile collects cell site location information ("CSLI"), which comprises the street address, longitude, and latitude of the cellular tower that carries a particular voice call, SMS message, or data session. This data is necessary for providing CMRS and CMDS, including network monitoring and maintenance, various aspects of billing, and routing emergency calls or text messages. Second, for purposes of operating our network, T-Mobile collects "timing advance" information, which identifies the

[1] As discussed in T-Mobile's response to the Commission's February 28, 2020, Notice of Apparent Liability for Forfeiture ("NAL"), FCC rules cover a limited subset of Geolocation Data. Although the Company responds more generally to your Inquiry, nothing in this letter should be considered a modification or waiver of any position taken in the Company's NAL response.

[2] *See, e.g.*, Cal. Civ. Code § 1798.140(ae)(1)(c) (defining "Sensitive personal information" to include a "consumer's precise geolocation"); *id.* § 1798.140(w) (defining "precise geolocation" as "data that . . . is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet"). For this response, T-Mobile includes all CSLI, irrespective of distance.

[3] Applications selected by the customer are independent of the carrier-customer relationship. For example, there are a wide variety of family locating and safety applications available from many other entities than T-Mobile, as well as some from T-Mobile, that interact with the customer's device for location information rather than relying on Geolocation Data.

historical location of a handset in the format of longitude and latitude coordinates, as corrected for certain measurement and transmission errors. Third, T-Mobile can access the current location of a handset to provide the estimated longitude and latitude (and, at times, elevation and/or street address) of the handset in response to either a customer placing a call or sending a text message to 911, as required by the Commission's E911 rules, or a "ping" from the Company.

1.b. *Please explain the reasons geolocation data is retained for both current and former subscribers.*

To operate our network and support customers, the Company must know where our customers' mobile devices are located. To that end, T-Mobile collects and retains Geolocation Data in connection with our essential operations. Examples include:

- Routing wireless communications,
- Providing customer support,
- Preventing or addressing signal interference,
- Operating and improving the Company's network,
- Detecting and preventing fraud,
- Routing emergency calls and texts, and informing emergency responders of the location from which a device originates an emergency call or text as required by the Commission's E911 rules,
- Preserving T-Mobile's legal interests, and
- Complying with applicable laws.

T-Mobile's policy is to seek affirmative customer consent before using Geolocation Data to provide any customer-requested service beyond CMRS or CMDS operations. When seeking consent from a customer, T-Mobile discloses the purposes for which their Geolocation Data will be used. The customer may revoke their affirmative consent at any time.

Beyond CMRS and CMDS, some of T-Mobile's family locating and safety services use Geolocation Data. Customers must provide their affirmative consent before their Geolocation Data is used for these services, which provide families with services, such as verifying that a family member arrived at an intended location and making the last known location of a participating device available if a family member goes missing. T-Mobile does not currently use Geolocation Data in connection with other services. T-Mobile's policy is not to collect or retain Geolocation Data for advertising purposes without affirmative customer consent.

Consistent with the FTC's guidance and industry best practices, T-Mobile's retention periods for Geolocation Data reflect business or legal needs and legal requirements. For example, T-Mobile is required to retain Geolocation Data associated with emergency calls for two years and has other security-related legal requirements for retention.

1.c. *How long is geolocation data retained for both current and former subscribers?*

Absent a legal hold, law enforcement preservation request, or other essential operations need, it is T-Mobile's policy to only retain Geolocation Data as follows:

- Current device location data collected in connection with necessary business operations for a transitory, brief period, except some opt-in family location and safety services that have longer retention periods reflecting customer needs when searching for a missing person.
- Timing advance data for a period of up to 90 days.
- CSLI for a period of up to 24 months.
- All Geolocation Data collected in connection with emergency calls for 2 years.

When a current customer closes her account, the Company deletes the information about the customer in the normal course under the Company's Records Management Policy.

1.d. *Please provide a description of what safeguards T-Mobile uses to protect current and former subscriber geolocation data.*

As our Privacy Notice explains, T-Mobile employs a holistic approach to safeguarding Geolocation Data from improper access, use, and disclosure. Among other measures: T-Mobile minimizes the amount of Geolocation Data in our possession or control. Absent affirmative customer consent, T-Mobile's policy is to collect Geolocation Data only for essential operations purposes, such as providing customers with mobile communication and internet access services, facilitating emergency calling services, and operating and maintaining our networks. T-Mobile further limits the privacy risks associated with Geolocation Data by retaining customer Geolocation Data only for as long as we have a legitimate business purpose or legal need or as applicable laws, regulations, or government orders require.

T-Mobile also protects Geolocation Data by employing a variety of physical, electronic, and procedural safeguards. For example, T-Mobile trains personnel on the importance of abiding by the Company's privacy policies and procedures. T-Mobile's privacy compliance team plays a key role in product and service development and ongoing operations, including conducting privacy impact assessments as part of our product design process and ensuring that the Company takes privacy and data protection into account as a matter of course. T-Mobile classifies Geolocation Data as among the most sensitive types of data we have, and as such requires it to be treated with technical safeguards that are appropriate to that sensitivity.

1.e. *In what country (or countries) is geolocation data stored?*

T-Mobile is a U.S.-based company and primarily stores Geolocation Data in the United States. T-Mobile does not store Geolocation Data outside the United States when doing so would violate a legal requirement, and takes national security concerns and legal requirements into consideration when making decisions related to overseas storage of Geolocation Data, including by prohibiting Geolocation Data storage in jurisdictions subject to U.S. export controls.

1.f. *Please share whether and how you disclose your data retention policies to subscribers.*

T-Mobile's Privacy Notice discloses that a customer's personal information (including Geolocation Data) is retained for a period determined by how long the Company reasonably needs it "for business or tax needs, or legal reasons."

1.g. *What is your data deletion policy for current or former subscribers, and how do you dispose of subscriber geolocation data?*

T-Mobile's practice is to delete Geolocation Data under the Company's Records Management Policy based on the time periods discussed above. We apply industry best practices for secure deletion when deleting Geolocation Data, such as logging deletions and auditing the process.

1.h. *Do your subscribers have any opportunity to opt-out of your data retention policies and if not, why not?*

T-Mobile primarily retains Geolocation Data for the periods described above in connection with the Company's essential operations. Because opting-out of continued retention could undermine our essential operations, we generally do not allow customers to opt-out of the Company's retention of Geolocation Data. As our Privacy Notice explains, we do allow customers to opt-out of the use of device diagnostic information—including Geolocation Data—for troubleshooting and network improvement.

2.a. *Please provide T-Mobile and Metro's process and policies for sharing subscriber geolocation data with law enforcement.*

Each year, T-Mobile publishes a detailed Transparency Report, available on T-Mobile's website, regarding responses to legal demands for customer information. As explained in those reports, T-Mobile provides Geolocation Data to U.S. law enforcement only when authorized or required to do so by law.

2.b. *Describe the arrangements, agreements, and circumstances in which T-Mobile and Metro share subscriber geolocation data with third parties that are not law enforcement.*

T-Mobile may disclose Geolocation Data to our service providers, and our practice is to require that they treat it in accordance with T-Mobile's instructions and to bar them from disclosing any Geolocation Data to third parties. T-Mobile may also disclose Geolocation Data where required by law or legal process, in connection with the provision of emergency response, or as necessary to protect T-Mobile's legal interests, such as disclosing it in a lawsuit where Geolocation Data is material and relevant, after seeking appropriate confidentiality protections. T-Mobile's practice is to obtain affirmative customer consent before sharing Geolocation Data in other circumstances. T-Mobile's practice is not to sell Geolocation Data to third parties. Our Privacy Notice notifies our customers of these practices.

2.c. *Describe in detail the process by which a subscriber may opt out of the sharing of their geolocation data. Under this opt-out process is that subscriber's data still shared with third parties? In particular, does the opt-out process allow a subscriber to opt-out of the sharing of their geolocation data with all third parties that are not law enforcement?*

As detailed above, T-Mobile's practice is that we do not sell Geolocation Data, and we obtain opt-in consent before sharing Geolocation Data in non-essential circumstances. These choices are explained in further detail in T-Mobile's Privacy Center. Customers may revoke such consent at any time.

2.d. *Are subscribers notified of the sharing of their geolocation information with third parties that are not law enforcement? And if so, how are they notified?*

Customers have ready access to the Company's Privacy Center, including its Privacy Notices, which provides easy-to-follow explanations of the circumstances in which the Company shares a customer's personal information, including Geolocation Data, with third parties.

In conclusion, T-Mobile is proud of its efforts to protect the privacy of our customers while providing the excellent service our customers demand. Again, thank you for your inquiry, and please do not hesitate to contact us if you have any further questions or concerns.

Sincerely,

Kathleen Ham
Senior Vice President, Government Affairs
T-Mobile USA, Inc.

cc: Commissioner Brendan Carr
Commissioner Geoffrey Starks
Commissioner Nathan Simington